PERSEREC

PERS-TR-94-001
OCTOBER, 1993

Assessment of Position Factors That Increase Vulnerability to Espionage

Kent S. Crawford
PERSEREC

Michael J. Bosshardt
PDRI, Inc.

Approved for Public Distribution:
Distribution Unlimited

Defense Personnel Security Research Center
99 Pacific Street, Building 455-E
Monterey, CA 93940-2481

PERS-TR-94-001 October 1993

Assessment of Position Factors That Increase Vulnerability to Espionage

Prepared by

Kent S. Crawford
Defense Personnel Security Research Center

Michael J. Bosshardt
Personnel Decisions Research Institutes, Inc.

Released by

Roger P. Denk
Director

Defense Personnel Security Research Center
Monterey, California 93940-2481

Executive Summary

To reduce the likelihood of espionage, personnel security programs have been implemented to prevent untrustworthy or unreliable individuals gaining access to classified information. These programs have ignored the role that factors such as geographic location of the position and degree of position oversight might play in increasing the likelihood of espionage. Position factors may increase the espionage vulnerability of the average position holder. The method for evaluating the degree to which these factors affect the likelihood of espionage for a position was labeled position vulnerability assessment (PVA).

The objectives of this study were to: (1) identify PVA factors and develop rating scales for each factor, (2) weight the importance of each factor, (3) develop a procedure for combining these factors to compute a PVA score for a position, and (4) assess the feasibility of implementing PVA. The study focused only on positions where the incumbent had access to sensitive compartmented information (SCI).

Forty-six counterintelligence personnel from 10 government agencies participated in the study. They identified and refined PVA factors, helped in developing rating scales, estimated the importance of each factor, and provided ideas concerning the potential usefulness of PVA.

The results of the questionnaire analyses and workshops yielded 18 PVA factors organized into the following four categories: (1) access and exposure to SCI and other classified/sensitive information (four factors), (2) job factors (five factors), (3) threats from potential contacts (three factors), and (4) security countermeasures (five factors). The four factors rated the most important were the sensitivity of information to which the individual had access, the amount of contact with foreign nationals, the frequency of access to SCI and other classified/sensitive information, and the job location threat.

Several issues were identified that should be examined before implementing PVA. First, there is a need to understand the relative importance of person characteristics and position factors in relation to espionage. Second, the extent to which PVA factors need to be tailored for different agencies and for groups with different access levels within an agency should be examined. Third, the most effective and efficient means of gathering and updating PVA scores need to be identified. Fourth, the cost-benefits of implementing PVA should be determined. Until such research is completed, allocating resources to implementing PVA is not warranted.

Nonetheless, this research has contributed to a broader perspective on the dynamics of espionage. This perspective should help security managers in the field examine and potentially reduce the vulnerability of some positions where this can be accomplished without adversely impacting on job performance.

Table of Contents

Executive Summary i
List of Tables iii
Introduction 1
Background 1
Research on Position Factors 1
Objectives 2
Methodology 3
Population 3
Identification of PVA Factors 3
Development of PVA Rating Scales 4
Results 5
PVA Factors and Rating Scales 5
A. Access and Exposure to SCI and other Classified/Sensitive Information 5
B. Job Factors 5
C. Threats from Potential Contacts 6
D. Security Countermeasures 6
PVA Factor Importance Weights 7
PVA Form Scoring Procedures 8
Implementation of Position Vulnerability Assessment 9
PVA Factors That Organizations Can Change 9
Person Characteristics and Position Factors 10
Feasibility of Implementing PVA 10
Conclusion 11
References 12
Endnotes 13
List of Appendixes 14

List of Tables

1. Mean Absolute and Relative Importance Ratings for Position Vulnerability Assessment Factors 7
2. Sum of Factor Weights Assigned to each Position Vulnerability Assessment Category 8
3. Comparison of Position Vulnerability Factors in Terms of Job Performance Requirements 9

Introduction

Background

Reducing the likelihood of espionage is a primary objective of personnel security programs in the intelligence community and Department of Defense (DoD). While these programs also help reduce the likelihood of inadvertent compromise, the significant failures usually occur when a cleared individual deliberately provides valuable classified or sensitive information to an adversary or competitor.

Personnel security programs have traditionally viewed likelihood of espionage from the perspective that individuals with certain characteristics are more likely to commit espionage. Examination of existing personnel security regulations (e.g., Department of Defense, 1987; Director of Central Intelligence, 1992) indicates that many personal characteristics have been identified as being of personnel security concern. Examples of such characteristics include alcohol abuse, drug abuse, emotional/mental disorders, and financial irresponsibility. For each characteristic, detailed criteria have been developed to specify what constitutes unacceptable levels of risk. Screening out individuals who meet the criteria on a given characteristic or characteristics enhances personnel security.

This focus has largely ignored the role that position factors may play in increasing the likelihood of espionage. Examples of position factors are geographic location of the job, level of security countermeasures associated with the job, and degree of position oversight. Position factors are not totally ignored in the current system. One factor, level of access to classified information required by the position holder, is used to determine the type of personnel security investigation the job incumbent receives. It also determines the amount of continuing evaluation (i.e., ongoing monitoring of individuals after they receive their clearance). The higher the level of access, the greater the expenditure of investigative and continuing evaluation resources. At issue in the current report is the role that position factors may play in contributing to the likelihood of espionage.

Research on Position Factors

Two recent reviews of continuing evaluation programs suggest that identifying position factors associated with vulnerability to espionage may be an important step for improving personnel security. DuBois, Bosshardt, and Crawford (1991) provided a detailed analysis of DoD continuing evaluation regulations, as well as regulations for four government-based personnel reliability programs. The authors concluded that the concept of position vulnerability assessment held promise for identifying personnel with a higher vulnerability to espionage. Heuer (1992) discussed whether more efficient and effective continuing evaluation programs can be developed using fewer resources. He concluded this is possible by targeting continuing evaluation efforts toward those at greatest risk. Targeting could be based on careful assessments of the security risk associated with various position characteristics, personal attributes, and background characteristics.

Examination of current theories of espionage provides additional support for the concept of position factors contributing to person vulnerability. In a 1990 study, Abbott and Rosenthal examined several theories of espionage and the implications of these theories from a position risk

perspective. Ties theory, incentive theory, and event theory were among the theories cited. Ties theory, which describes how individuals can be tied or befriended to other people or institutions, implies that position location may be associated with espionage. Incentive theory, which describes how disloyalty may occur when expected benefits exceed expected risk, suggests that economic or position cost-of-living factors may influence espionage risk. Event or situation theory, which implies that individuals have characteristics that can be affected by certain events and environments, implies that job-related travel and other position variables *(*e.g., job stress) may impact on espionage risk. Thus, these and other theories of espionage suggest that position factors can impact on likelihood of espionage.

Findings from a world-wide survey of continuing evaluation practices at 60 military installations (Bosshardt, Dubois, Crawford, & McGuire, 1991; Bosshardt, DuBois, & Crawford, 1991a; Bosshardt, DuBois, & Crawford, 1991b; DuBois, et al., 1991) provide more evidence supporting the position vulnerability concept. The survey results indicated that only 45 percent of the installations sampled targeted more continuing evaluation resources toward certain positions. Nearly all these targeting efforts were based entirely on level of access rather than also including other specific position factors. One key recommendation given by security managers was to devote more continuing evaluation emphasis to persons in certain positions and geographical areas.

Very few attempts have been made to specifically identify position factors associated with espionage risk. One exception was the study by Abbott and Rosenthal (1990) which resulted in a preliminary instrument for assessing position vulnerability factors. These authors identified nine position characteristics *(*e.g., sustained accessibility of foreign agents to position incumbent, routine access to sensitive information) that were hypothesized to relate to position risk for naval personnel with SCI access. A sample of positions were then rated on each characteristic. For each position, ratings on the position characteristics were weighted and summed to create a total risk score.

Although this study provides a useful starting point for examining the position risk, it had at least two limitations. First, the personnel used to identify factors and factor weights lacked extensive knowledge of counterintelligence and recruitment of spies. Second, the findings were restricted to a limited number of cleared positions in one Navy command. The present study built upon the Abbott and Rosenthal research by using counterintelligence personnel from a much larger sample of government organizations. This would allow for the identification of more generalizable position risk factors and result in greater expert input.

Objectives

The primary purpose of this study was to identify factors that impact on the espionage vulnerability of incumbents of different positions. The method for evaluating the degree to which these factors affect the likelihood of espionage was labeled *position vulnerability assessment* (PVA). More specifically, this project required completing the following four objectives:

1. Identify PVA factors and develop rating scales for each factor.
2. Weight the importance of each factor.

3. Develop a procedure for combining these factors and computing a PVA score for a position.
4. Assess the feasibility of implementing PVA.

Methodology

Population

The specific focus of this study was on positions where incumbents had access to SCI. This population was chosen for the following reasons: (a) this group represented a useful starting point for identifying PVA factors and evaluating PVA, (b) espionage within this population has extremely serious consequences for national security, (c) PVA could more realistically be expected to be implemented in the intelligence community, and (d) individuals with SCI access operate under a common set of policies even though they are located in different agencies.

Identification of PVA Factors

The first step in the development of a PVA form was to identify position characteristics or factors that are related to vulnerability to espionage. This process involved three steps: (1) reviewing relevant literature, (2) conducting a questionnaire survey to revise the initial list of PVA factors, and (3) meeting with counter-intelligence experts to further refine the list of PVA factors. Each step is described below.

Literature review. The process of identifying PVA factors was begun by reviewing available literature and materials on espionage cases and espionage prevention. These literature review procedures included: (a) conducting computerized searches using the PsycINFO data bases, (b) contacting researchers who are active in the personnel security field, (c) examining personnel security manuals from various government agencies, (d) checking references cited in relevant technical reports, and (e) examining variables included in PERSEREC's espionage database. Source materials reviewed included technical reports, government publications, personnel security manuals, and newspaper articles. Several of these sources described case histories of individuals who were convicted of espionage. Overall, the review process resulted in the examination of over 100 sources, 40 of which provided one or more possible PVA factors. More than 100 possible PVA factors were identified.

This large number of possible PVA factors was reduced using a two-step procedure. First, factors were eliminated that focused primarily on personal characteristics *(*e.g.*,* frequency of substance abuse) rather than on position characteristics *(*e.g., availability of employee assistance programs). The remaining factors were then sorted into general categories based on similar content *(*e.g.*,* items related to employee assistance programs). This process produced an initial list of 17 PVA factors.

Questionnaire survey. After identifying this preliminary set of PVA factors, a questionnaire was developed to obtain information about these and other possible factors. This questionnaire asked respondents to (a) evaluate the importance of these preliminary PVA factors, (b) revise, where necessary, the wording of these factors, (c) combine related factors, and (d) add new factors.

In September, 1991, this questionnaire was mailed to 10 representatives from 10 government agencies with intelligence missions. Each person was asked to have five counterintelligence experts from that organization complete the questionnaire. Forty-six counterintelligence experts from nine government agencies returned completed questionnaires.[1] Besides rating the importance of each PVA factor, respondents made several suggestions for revising the PVA factor list. Based on these survey comments, several revisions were made. Respondents also provided comments on issues associated with implementing a PVA approach.

Workshop with counterintelligence experts. After revising the list of PVA factors, a meeting was held with 11 counterintelligence experts from nine government agencies in Washington, DC, to further refine these PVA factors and to gather additional information about their relative importance. Appendix A lists the workshop participants and their organizational affiliation.

Development of PVA Rating Scales

After identifying and defining a set of PVA factors, rating scales were developed to assess each factor. This process involved two steps: (1) conducting a questionnaire survey and (2) meeting with counterintelligence experts. Each step is described below.

Questionnaire survey. The first step in developing a set of PVA rating scales was to obtain examples that described very high, moderate, and very low vulnerability to espionage levels for each PVA factor. This was accomplished using a questionnaire survey. Specifically, for each PVA factor, questionnaire respondents were asked to write one or two short examples that characterized a position at very high vulnerability from an espionage standpoint, one or two examples that described a position at moderate vulnerability, and one or two examples that characterized a position at very low vulnerability.

This questionnaire was mailed to the 11 persons who attended the earlier PVA workshop. Each person was asked to have two persons from that agency complete the questionnaire. Fifteen counterintelligence experts from seven government agencies with intelligence missions returned completed questionnaires.[2] Summarization of results from the questionnaires resulted in a preliminary set of rating scales. There was one scale per PVA factor with each rating scale defined at five levels with specific examples.

Second workshop with counterintelligence experts. After developing a preliminary set of PVA rating scales, a meeting was held with seven counterintelligence experts from seven government agencies in Washington, DC, to revise these scales. Appendix B lists the persons who attended this workshop and their organizational affiliation. During this workshop, final revisions were made to the PVA factors and scales.

Workshop participants also rated the absolute and relative importance of these PVA factors. Importance was defined as the degree to which the factor would make a position holder vulnerable to being recruited for or volunteering for espionage. For the absolute importance ratings, participants were asked to distribute 100 points across the 18 factors such that the sum of the individual factors weights totaled 100. In the relative ratings, the participants assigned an importance rating of 1 (very unimportant) to 5 (very important) to each factor. Besides the seven persons who attended the workshop, two individuals who attended the earlier PVA workshop also provided ratings following the workshop.

Results

This section presents the results from the PVA developmental work described in the previous section. Details are presented below according to the following topics: (1) PVA factors and rating scales, (2) PVA Factor Importance Weights, and (3) PVA form scoring procedures.

PVA Factors and Rating Scales

The final results from the questionnaire analyses and workshops yielded 18 PVA factors that were organized into the following four categories: (1) Category A - Access and exposure to SCI and other classified/sensitive information (four factors), (2) Category B - Job factors (five factors), (3) Category C - Threats from potential contacts (three factors), and (4) Category D - Security countermeasures (six factors). The specific factors and their definitions are presented below. Rating scales for each factor are presented in Appendix C.

A. Access and Exposure to SCI and other Classified/Sensitive Information

1. **Frequency of Access to Classified/Sensitive Information**. This factor refers to the frequency with which access to SCI and/or other classified/sensitive information is required to perform job duties. Such information could include classified, mission-critical, economically sensitive, or technologically critical information.
2. **Range/Amount of Access to Classified/Sensitive Information**. This factor refers to the range and amount of SCI and/or other classified/sensitive information (including number of compartments) the position holder handles, has access to, or knowledge of.
3. **Sensitivity of Classified/Sensitive Information**. This factor refers to the value of SCI and/or other classified/sensitive information that the position holder has access to with regard to its usefulness to potential adversaries, risk to human life, or economic consequences if the information is compromised.
4. **Potential for Unauthorized Exposure to Classified/Sensitive Information**. This factor refers to the job requirements and characteristics (e.g., authority, contacts, or proximity to classified information) associated with the position that would enable the position holder to obtain access to classified/sensitive information that the individual does not have a need to know.

B. Job Factors

1. **Career Field**. This factor refers to the general career field (e.g., communications, cryptography, clerical) for this position. It assumes that the position requires SCI access.
2. **Position Oversight**. This factor refers to the amount of time spent working alone with classified materials, and the degree and type of supervisory oversight of the position. This includes evening, night, or weekend hours.
3. **Position Status**. This factor refers to the extent to which the position does not provide opportunities for status, advancement, recognition, and challenge.
4. **Position Stress**. This factor refers to the extent to which the position is likely to cause a typical position holder to feel stress due to job pressures, demands, and short deadlines.

This stress can sometimes lead to other problems (e.g., alcohol abuse) that increase vulnerability.

5. **Cost-of-Living/Compensation Pressures**. This factor refers to the extent to which the salary for this position is commensurate with the cost of living associated with the work location.

C. Threats from Potential Contacts

1. **Contact With Foreign Nationals**. This factor refers to the extent to which the duties of this position involve or facilitate contacts with individuals located in or visiting from foreign countries.
2. **Job Location Threat**. This factor refers to the known foreign intelligence threat associated with the geographic location of the position. Threat is associated with the intensity of local foreign intelligence and with location distance.
3. **Temporary Additional Duty (TDY) Travel**. This factor refers to the amount and types of TDY travel associated with this position and the destinations typically visited.

D. Security Countermeasures

1. **Information Security Safeguards and Procedures**. This factor refers to the extent and quality of information security *(*e.g., classified materials controls, open storage rules) in the unit and work location.
2. **Physical Security Safeguards and Procedures**. This factor refers to the extent and quality of physical security *(*e.g., facilities and building access controls, exit searches, visibility of guard force, external security measures) in the unit and work location.
3. **Personnel Security Procedures**. This factor refers to the extent and quality of personnel security procedures associated with this position (e.g., personnel security investigations, drug testing, polygraph, continuing evaluation procedures).
4. **Security Education Procedures**. This factor refers to the extent and quality of security education (e.g., security awareness briefings, threat briefings, counterintelligence briefings) in the organization and work unit.
5. **Employee Assistance Programs**. This factor refers to the extent and quality of employee assistance programs (e.g., alcohol, drug, family, financial, etc.) available to the position holder.
6. **Availability of Support Systems**. This factor refers to whether there are family members, coworkers, or other English-speaking personnel in the geographic location of the position. These persons could provide a support system for position holders by allowing them to discuss interests and problems.

PVA Factor Importance Weights

Means and standard deviations for the two importance ratings of the different PVA factors are shown in Table 1. The rank ordering of factors was similar in both lists. Examination of the standard deviations for the absolute ratings suggests that ratings for some PVA factors are more variable than for other factors. High standard deviations indicate differences in expert ratings concerning the importance of a particular factor. Factors with relatively high variability are sensitivity of classified/sensitive information, contact with foreign nationals, personnel security procedures, and frequency of access to classified/sensitive information. Factors with relatively low variability are physical security safeguards and procedures, job location, cost of living/compensation pressures, position status, and position stress.

Table 1

Mean Absolute and Relative Importance Ratings for Position Vulnerability Assessment Factors

Absolute Importance Rating		Relative Importance Rating		Position Vulnerability Assessment Factor Rank Ordered by Mean Absolute Importance Rating
Mean	**SD**	**Mean**	**SD**	
9.59	5.06	4.17	.87	A3. Sensitivity of Classified/Sensitive Info.
8.54	3.66	4.39	.70	C1. Contact with Foreign Nationals
7.73	3.57	3.89	.78	A1. Frequency of Access to Classified/Sensitive Info.
7.73	1.41	4.22	.83	C2. Job Location Threat
7.38	2.78	4.00	.87	B1. Career Field
7.38	2.91	3.89	.60	A2. Range/Amount of Classified/Sensitive Info.
6.79	3.61	3.94	.95	D3. Personnel Security Procedures
5.50	2.54	3.72	.97	D1. Information Security Safeguards and Procedures
5.04	1.72	3.61	.60	B5. Cost of Living/Compensation Pressures
4.45	1.20	3.56	1.01	D2. Physical Security Safeguards and Procedures
4.33	2.57	3.22	.67	C3. TDY Travel
4.22	2.45	3.44	.88	D4. Security Education Procedures
4.22	2.00	3.17	.94	B2. Position Oversight
4.10	1.76	3.50	.79	B3. Position Status
3.62	2.60	2.50	.50	A4. Potential for Unauthorized Exposure to Classified /Sensitive Information
3.28	2.26	3.33	1.12	D6. Availability of Support Systems
3.05	1.76	3.00	1.22	B4. Position Stress
3.05	2.09	3.00	.71	D5. Employee Assistance Program

Notes. Absolute importance ratings were the result of allocating 100 points across the 18 factors; relative importance ratings were made on 1 to 5 scale. N = 9 raters

Table 2 compares the sums of the absolute importance weights of the individual factors within the different categories. Category A, Access and Exposure to Classified/Sensitive Information, had the highest weight (28.32); however, there are not large differences across the categories. Overall, the results suggest that each of the four areas represents an important domain in determining the espionage vulnerability of positions.

Table 2

Sum of Factor Weights Assigned to each Position Vulnerability Assessment Category

Category	Number of Factors	Sum of Factor Weights
A. Access and Exposure to SCI and other Classified/Sensitive Information	4	28.32
B. Job Factors	5	23.79
C. Threats from Potential Contacts	3	20.60
D. Security Countermeasures	6	27.29
Totals	**18**	**100.00**

PVA Form Scoring Procedures

After identifying the final PVA factors and rating scales, scoring procedures were developed for the PVA form. The objective was to combine the PVA factor scores into an overall or total score that could be used to compare the vulnerability of different positions.

As a first step in developing a scoring system, the mean importance ratings were examined to decide whether the PVA factors should be differentially weighted. Given the large differences between the weights assigned to different factors, the mean absolute importance ratings (shown in Table 1) were used as the basis for weighing each PVA factor. The mean absolute ratings, which had been provided by a diverse panel of counterintelligence experts, best represented the importance of the various PVA factors.

Once a position has been rated on a factor using the 5-point rating scale, a weighted factor score can be computed by multiplying the weight for a factor by the factor's rating. Finally, a total score can be computed for assessing the vulnerability of a particular position by summing the scores on all PVA factors. However, since the sum of the PVA factor weights was 100 and the maximum score for each factor was 5, the maximum total score would be 500 and the minimum 100. To simplify the interpretation of these total scores, a linear transformation formula was developed that resulted in scores ranging from 100 (highest level of vulnerability, all fives on each factor) to 0 (lowest level of vulnerability, all ones on each scale).

To simplify the process of assessing position vulnerability and computing PVA scores for different positions, a computerized format of the PVA form was developed. This computerized version can also store relevant information for many different positions and can be modified to include revised factors and/or different factor importance weights.[3]

Implementation of Position Vulnerability Assessment

The primary purpose of this report was to identify factors that affect the espionage vulnerability of incumbents of positions requiring SCI access. However, an attempt was also made to assess issues associated with implementing PVA.

PVA Factors That Organizations Can Change

One possible use of PVA would be to change position factors that contribute to high vulnerability. Certain factors are an inherent part of the job and cannot be easily changed without reducing the job performance of the incumbent. On the other hand, organizations have more leverage over other factors.

Table 3 presents a categorization of vulnerability factors over which managers have greater or lesser control in terms of their direct linkage to job performance requirements. The nine relatively fixed factors appear to account for approximately 58 percent of the total importance weights while those that the organization could more easily change account for 42 percent of the weight. These data suggest that managers could reduce vulnerability by changing the job conditions associated with the factors shown in the bottom half of the table.

Table 3

Comparison of Position Vulnerability Factors in Terms of Job Performance Requirements

Factors That Managers Cannot Easily Change	Weight
A3. Sensitivity of Classified/Sensitive Information	9.59
C1. Contact with Foreign Nationals	8.54
C2. Job Location Threat	7.73
A1. Frequency of Access to Classified/Sensitive Information	7.72
A2. Range/Amount of Access to Classified/Sensitive Information	7.38
B1. Career Field	7.38
B5. Cost of Living/Compensation Pressures	5.04
C3. Temporary Additional Duty (TDY) Travel	4.33
Total	**57.71**
Factors That Managers Can More Easily Change	**Weight**
D3. Personnel Security Procedures	6.79
D1. Information Security Safeguards and Procedures	5.50
D2. Physical Security Safeguards and Procedures	4.45
B2. Position Oversight	4.22
D4. Security Education Procedures	4.22
B3. Position Status	4.10
A4. Potential for Unauthorized Exposure to Classified/Sensitive Information	3.63
D6. Availability of Support Systems	3.28
D5. Employee Assistance Programs	3.05
B4. Position Stress	3.05
Total	**42.29**

Person Characteristics and Position Factors

Both person characteristics and position factors contribute to vulnerability to espionage. This report has identified position factors and each of their relative contributions to overall position vulnerability. Nonetheless, from a resource allocation perspective, a fundamental issue remains. What contributes more to vulnerability—person characteristics or position factors? Also, is the interaction between the two areas (i.e., certain types of individuals in certain types of positions) more critical then either area alone in contributing to vulnerability?

It was beyond the scope of this study to examine either the relative importance of person characteristics and position factors or the interaction between the two areas. Nonetheless, in an era of shrinking resources, implementing new approaches in personnel security will require decreasing the resources devoted to other areas. Lacking information on the relative importance of person characteristics and position factors, we cannot determine whether reallocating resources to more of a PVA approach would reduce the overall likelihood of espionage and be a cost-effective improvement over the current system.

Feasibility of Implementing PVA

There are several issues that need to be resolved before implementing PVA. Three key issues are discussed below.

Generalizability of current PVA factors and weights. The degree to which the PVA factors identified in this study would be the best set to use in any given agency is unclear. The focus of this study was to identify a comprehensive set of PVA factors and weights for positions in which the incumbents have access to SCI. Counterintelligence personnel who served as subject matter experts represented a wide range of organizations that had intelligence missions or intelligence subunits. Therefore, the factors and weights identified in this study may not be the most effective ones to use in a given agency or unit within an agency.

Each government agency has special requirements, missions, and personnel. PVA may need to be tailored for specific agency applications. The approach used in this study could be used to develop agency-specific forms with more or fewer factors, modified rating scales, and different importance weights. It is unclear at this time whether there would be large differences between these forms and the more generic form developed in this study.

A final generalizability issue concerns the level of access for the targeted population. The current study focused on positions where individuals have access to SCI. It is possible that even within the same agency, factors and factor weights may differ when the positions being considered only require access to Top Secret or Secret information.

Difficulty of obtaining PVA ratings. It may be difficult to gather and update PVA ratings since doing so requires very detailed knowledge of local job conditions. Therefore, agencies could not use centralized data bases or headquarters personnel to make PVA ratings. Instead, a more decentralized rating process using field personnel would have to be implemented. This requirement would increase the administrative costs of implementing PVA.

Additionally, it is not clear how frequently positions would have to be rated. Some factors (e.g., cost of living, job location threat) might be relatively constant across time whereas other factors (e.g., position stress, TDY travel) could change as job requirements are modified. The

greater the extent to which job factors change, the more frequently PVA scores would have to be updated.

Difficulty in incorporating PVA into a personnel security program. Given the diversity of organizations and positions within an agency, it may be difficult to effectively incorporate PVA into a personnel security program. For example, one potential use for PVA would be to identify positions with high vulnerability and then screen and more closely reinvestigate individuals who will occupy these positions. However, this use of PVA is complicated by the fact that in many agencies, and DoD in particular, most individuals transfer positions frequently. Individuals can move from high vulnerable to low vulnerable positions. Thus, it would be very difficult to coordinate initial screening and periodic reinvestigations with PVA and assignment procedures.

Another application could be to enhance continuing evaluation procedures and security education for individuals occupying highly vulnerable positions. Procedures would be linked to the position and not the individual, thereby mitigating the problems discussed above. However, if there were considerable variability in the vulnerability of positions, it would require significant administrative effort to implement different continuing evaluation and security education programs with the same organizational unit or subunits.

Conclusion

The primary purpose of this report was to identify position factors that impact on the espionage vulnerability of incumbents of positions where individuals had access to SCI. This overall objective was accomplished through the identification of 18 PVA factors including rating scales and importance weights for different factors. Several issues remain to be solved before implementing PVA as a component of a personnel security system.

Additional research is required in the following areas: (1) the relative importance of person characteristics versus position factors in relation to espionage, (2) the extent to which PVA factors need to be tailored for different agencies and for groups with different access levels within an agency, (3) the most effective and efficient means of gathering and updating PVA scores, and (4) the cost-benefits of implementing PVA.

Nonetheless, this research has identified a number of position factors that could increase the likelihood of espionage, independent of the unique characteristics of any given position holders. These factors deserve consideration in our attempts to understand espionage. Knowledge of these factors should help security managers in the field a framework for examine and potentially reduce the vulnerability of some positions where this can be accomplished without adversely impacting on job performance.

References

Abbott, P.S., & Rosenthal, D.B. (1990). *Development of the position vulnerability assessment (PVA) instrument* (Draft Final Report 90-02). Alexandria, VA: HumRRO International, Inc.

Bosshardt, M.J., DuBois, D.A., & Crawford, K.S. (199la). *Continuing assessment of cleared personnel in the military services: Report 3 - Recommendations* (PERS-TR-91003). Monterey, CA: Defense Personnel Security Research and Education Center.

Bosshardt, M.J., DuBois, D.A., & Crawford, K.S. (199lb). *Continuing assessment of cleared personnel in the military services: Report 4 - System issues and program effectiveness* (PERS-TR-91-004). Monterey, CA: Defense Personnel Security Research and Education Center.

Bosshardt, M.J., DuBois, D.A., Crawford, K.S., & McGuire, D. (1991). *Continuing assessment of cleared personnel in the military services: Report 2 - Methodology, analysis, and results* (PERS-TR-91-002). Monterey, CA: Defense Personnel Security Research and Education Center.

Department of Defense (1987). *Personnel security program regulation* (DoD 5200.2-R). Washington, D.C.: Office of the Deputy Under Secretary of Defense for Policy.

Director of Central Intelligence (1992). *Personnel security standards and procedures governing eligibility for access to sensitive compartmental information* (Directive No. 1/14).

DuBois, D.A., Bosshardt, M.J., & Crawford, K.S. (1991). *Continuing assessment of cleared personnel in the military services: Report 1 - A conceptual analysis and literature review* (PERS-TR-91-001). Monterey, CA: Defense Personnel Security Research and Education Center.

Heuer, R. J., Jr. (1992). *Achieving more with less: An ideal continuing evaluation program.* Working paper prepared for the Office of Security, Central Intelligence Agency.

Endnotes

1. All of the respondents held security clearances, with 38 having SCI access eligibility, three having a Top Secret clearance, and five having a Secret clearance. Respondents had held their security clearances an average of 20.9 years. They averaged 16.5 years of experience in the security field and 10.0 years of experience in the counterintelligence field.

2. All of the respondents held security clearances; 13 had SCI access and two had Secret access. The respondents averaged 10 years of experience in the security field and 8.3 years of experience in the counterintelligence field. The questionnaire respondents wrote nearly 2,000 rating scale anchors. Because of the large number of anchors, it was necessary to develop rating scale anchors that summarized the content of several examples. To accomplish this, the anchors were sorted according to PVA factor, scale level (very high, moderate, very low), and content similarity. Five anchors (very high, high, moderate, low, and very low) were then developed for each PVA factor. Five anchors rather than three were used to obtain finer distinctions in the rating scale and to capture more of the diversity in content of the PVA factor.

3. This computer program entitled “Position Vulnerability Assessment” was developed for use on IBM compatible PCs with EGA or VGA displays. The program was designed to run under MS-DOS as a single-user, stand-alone program. There is no plan at this time to develop a multi-user version, but a version for Microsoft Windows has also been completed.

   Since the program would not be used on a frequent basis, it was critical that it be as user-friendly as possible. For this reason, a graphic user interface was employed using standard keyboard and mouse definitions found in Microsoft Windows. This would ensure that first-time users who are familiar with the Windows environment would be able to use the program with no difficulty. In addition, context-sensitive help and general help screens are provided. Thus, even users who are not familiar with the Windows environment can learn to use the program in a short time.

   The program provides windows for entering (a) the name of the rater, (b) information on the position and the organization, and (c) ratings on each of the 18 factors. When ratings have been entered for all 18 factors, the user can select a menu option to display a summary of the ratings plus the overall PVA score. The remaining features currently in development for the program are (a) a module for printing the summary of ratings and PVA score, and (b) a database module for saving and retrieving the data.

   Since the PVA form and scoring system were designed as a prototype, in practice, organizations may add or eliminate factors or may use different factor weights. All that is necessary to do this is to specify a set of factors and a set of weights for these factors. A computer program could then automatically transform these input factor weights into transformed weights.

List of Appendixes

A. Position Vulnerability Workshop Participants (4 February 1992)

B. Position Vulnerability Workshop Participants (14 May 1992)

C. Position Vulnerability Rating Scales

APPENDIX A

Position Vulnerability Workshop Participants
(4 February 1992)

David W. Ader
Department of Defense

Reid P. Broce
Federal Bureau of Investigation

Steven J. Brown
Department of Energy

Brian F. Dunne
Office of Personnel Management

Tom Husband
Office of the Assistant Secretary of Defense

David M.
Central Intelligence Agency

Linda S. Matthews
Department of the Army

Philip W. McMaster
Naval Investigative Service Command

Neely Moody
Defense Intelligence Agency

Jim Moree
U.S. Air Force

Peter Van Lannen
Department of State

APPENDIX B

Position Vulnerability Workshop Participants
(14 May 1992)

David W. Ader
Department of Defense

Reid P. Broce
Federal Bureau of Investigation

Steven J. Brown
Department of Energy

Brian F. Dunne
Office of Personnel Management

Tom Husband
Office of the Assistant Secretary of Defense

David M.
Central Intelligence Agency

Philip W. McMaster
Naval Investigative Service Command

APPENDIX C

Position Vulnerability Rating Scales

A. Access and Exposure to Classified/Sensitive Information

A1. **Frequency of Access to Classified/Sensitive Information** . This factor refers to the frequency with which access to SCI and/or other classified/sensitive information is required to perform job duties. Such information could include classified, mission-critical, economically sensitive, or technologically critical information.

1. Position requires very infrequent access to SCI and/or other classified/sensitive information *(*e.g., less than once per month).
2. Position requires infrequent access to SCI and/or other classified/sensitive information *(*e.g., about once per month or a few times per month).
3. Position requires somewhat frequent access to SCI and/or other classified/sensitive information *(*e.g., about once per week or a few times per week).
4. Position requires frequent access to SCI and/or other classified/sensitive information *(*e.g., at least once per day).
5. Position requires continuous access to SCI and /or other classified /sensitive information *(*e.g., on a continuous basis).

A2. **Range/Amount of Access to Classified/Sensitive Information** . This factor refers to the range and amount of SCI and/or other classified/sensitive information (including number of compartments) the position holder handles, has access to, or knowledge of.

1. Position holder typically handles, has access to, or knowledge of a very small range/amount of SCI and/or other classified/sensitive information *(*e.g., single compartment, single source, single system, single SAP).
2. Position holder typically handles, has access to, or knowledge of a small range/amount of SCI and/or other classified/sensitive information.
3. Position holder frequently (but not continually) handles, has access to, or knowledge of a moderate range/amount of SCI and/or other classified/sensitive information.
4. Position holder continually handles, has access to, or knowledge of a large range/amount of SCI and/or other classified/sensitive information.
5. Position holder continually handles, has access to, or knowledge of a very large range/amount of SCI and/or other classified/sensitive information *(*e.g., multiple compartments, multiple sources, multiple systems, multiple SAPs).

A3. **Sensitivity of Classified/Sensitive Information**. This factor refers to the value of SCI and/or other classified/sensitive information that the position holder has access to with regard to its usefulness to potential adversaries, risk to human life, or economic consequences if the information is compromised.

1. Position holder typically has access to SCI and/or other classified information that has limited value to potential adversaries or competitors and for which compromise of the information would have very limited consequences.
2. Position holder typically has access to SCI and/or other classified information that has some value to potential adversaries or competitors and for which compromise of the information would have limited consequences.
3. Position holder typically has access to SCI and/or other classified information that has moderate value to potential adversaries or competitors and for which compromise of the information would have moderate consequences.
4. Position holder typically has access to SCI and/or other classified information that has high value to potential adversaries or competitors and for which compromise of the information would have adverse consequences.
5. Position holder typically has access to SCI and/or other classified information that has extremely high value to potential adversaries or competitors and for which compromise of the information would have extremely adverse or permanent consequences.

A4. **Potential for Unauthorized Exposure to Classified/Sensitive Information**. This factor refers to the job requirements and characteristics *(*e.g., authority, contacts, or proximity to classified information) associated with the position that would enable the position holder to obtain access to classified/sensitive information that the individual does not have a need to know.

1. Position holder has very low potential for unauthorized exposure to classified/sensitive information *(*e.g., position has relatively low authority, involves few close contacts with persons having SCI or other sensitive access, or is not very close to moderate amounts of classified information).
2. Position holder has low potential for unauthorized exposure to classified/sensitive information *(*e.g., position has moderate authority, involves relatively few close contacts with persons having SCI or other sensitive access, or is relatively close to moderate amounts of classified information).
3. Position holder has moderately high potential for unauthorized exposure to classified/sensitive information *(*e.g., position has moderately high authority, involves some close contacts with persons having SCI or other sensitive access, or is close to moderate amounts of classified information).
4. Position holder has high potential for unauthorized exposure to classified/sensitive information (e.g., position has high authority, involves several close contacts with persons having SCI or other sensitive access, or is close to large amounts of classified information).
5. Position holder has very high potential for unauthorized exposure to classified/sensitive information *(*e.g., position has extremely high authority, involves numerous close contacts with persons having SCI or other sensitive access, or is very close to large amounts of classified information).

B. Job Factors

B1. **Career Field**. This factor refers to the general career field *(*e.g., communications, cryptography, clerical) for this position. It assumes that the position requires SCI access.

1. Low vulnerability career field *(*e.g., supply personnel).
2. Somewhat vulnerable career field *(*e.g., security professionals, librarians, drivers, maintenance personnel, security guards, support personnel).
3. Moderately vulnerable career field *(*e.g., analysts, counterintelligence professionals, engineers, investigators, managers, administrative personnel, military officers, military enlisted personnel, production workers).
4. Very vulnerable career field *(*e.g., case, collection, operation, or report officers, scientists, secretaries / clerks, linguists / translators).
5. Extremely vulnerable career field *(*e.g., telecommunications personnel, cryptographical personnel).

B2. **Position Oversight**. This factor refers to the amount of time spent working alone with classified materials, the degree and type of supervisory oversight of the position. This includes evening, night, or weekend hours.

1. Position holder does not work alone with classified materials.
2. Position holder rarely works alone with classified materials or for very brief time periods with little or no supervisory oversight.
3. Position holder occasionally works alone with classified materials or for limited time periods with little or no supervisory oversight.
4. Position holder frequently works alone with classified materials or for extended time periods with little or no supervisory oversight.
5. Position holder always works alone with classified materials with no supervisory oversight.

B3. **Position Status**. This factor refers to the extent to which the position does not provide opportunities for status, advancement, recognition, and challenge.

1. Position has high status, opportunities for rapid advancement, high recognition for achievements, and considerable challenge.
2. Position has relatively high status, opportunities for relatively rapid advancement, recognition for achievements, and challenging work.
3. Position has moderate status, some opportunities for advancement, occasional recognition for achievements, and some challenge.
4. Position has low status, slow or limited opportunities for advancement, little recognition for achievements. and little challenge.
5. Position has very low status, no opportunities for advancement, very little or no recognition for achievements, and very limited challenge.

B4. **Position Stress**. This factor refers to the extent to which the position is likely to cause a typical position holder to feel stress due to job pressures, demands, and short deadlines. This stress can sometimes lead to other problems (e.g., alcohol abuse) that increase vulnerability

1. Position is not at all stressful. Position involves little or no pressure, a workload that is neither excessive nor inadequate, normal hours, and no required overtime. Position holder never has to rush to meet deadlines.
2. Position is slightly stressful. Position involves relatively little pressure, a workload that is generally neither excessive nor inadequate, normal hours, and very little or no required overtime. Position holder rarely must rush to meet deadlines.
3. Position is moderately stressful. Position involves some pressure, a workload that is sometimes excessive or sometimes inadequate, occasional long hours, and only infrequent required overtime. Position holder occasionally must rush to meet deadlines.
4. Position is very stressful. Position involves occasional heavy pressure, a workload that is often excessive or excessively low, moderately long hours, and some required overtime. Position holder sometimes must rush to meet deadlines.
5. Position is extremely stressful. Position involves continual heavy pressure, an excessive workload, very long hours, and considerable required overtime. Position holder frequently must rush to meet short deadlines.

B5. **Cost of Living/Compensation Pressures**. This factor refers to the extent to which the salary for this position is commensurate with the cost-of-living associated with the work location.

1. Position holder's salary and other compensation is very high compared to the cost-of-living associated with the work location.
2. Position holder's salary and other compensation is high compared to the cost-of-living associated with the work location.
3. Position holder's salary and other compensation is about average compared to the cost-of-living associated with the work location.
4. Position holder's salary and other compensation is low compared to the cost-of-living associated with the work location.
5. Position holder's salary and other compensation is very low compared to the cost-of-living associated with the work location.

C. Threats from Potential Contacts

C1. **Contact with Foreign Nationals**. This factor refers to the extent to which the duties of this position involve or facilitate contacts with individuals located in or visiting from foreign countries.

1. Position holder has no contact with foreign nationals.
2. Position holder has infrequent and/or very casual contact with high threat foreign nationals.
3. Position holder has somewhat frequent and/or casual contact with high threat foreign nationals.
4. Position holder has frequent and/or close contact with high threat foreign nationals.
5. Position holder has very frequent and/or very close contact with high threat foreign nationals.

C2. **Job Location Threat**. This factor refers to the known foreign intelligence threat associated with the geographic location of the position. Threat is associated with the intensity of local foreign intelligence and with location distance.

1. Medium/low threat U.S. Locations. U.S. Locations where the foreign intelligence threat is less intense.
2. High threat U.S. Locations. U.S. Locations where the foreign intelligence threat is very intense (e.g., Washington DC, New York City, San Francisco).
3. Medium/low threat overseas locations. Overseas locations where the foreign intelligence threat is less intense *(*e.g., Toronto, Sydney).
4. High threat overseas locations. Overseas locations where the foreign intelligence threat is intense (e.g., Mexico City, Vienna).
5. Critical threat overseas locations. Overseas locations where the foreign intelligence threat is very intense (e.g., Moscow, Beijing).

C3. Temporary Additional Duty (TDY) Travel . This factor refers to the amount and types of TDY travel associated with this position and the destinations typically visited.

1. Position does not require any TDY travel.
2. Position requires short TDY travel to medium/low threat overseas areas *(*e.g., Toronto, Sydney) or lengthy TDY travel within the U.S.
3. Position requires lengthy TDY travel to medium/low high threat overseas areas *(*e.g., Toronto, Sydney).
4. Position requires TDY travel to any high threat overseas area *(*e.g., Mexico City, Vienna) or extended TDY travel to overseas countries.
5. Position requires TDY travel to any critical threat overseas area *(*e.g., Moscow, Beijing).

D. Security Countermeasures

D1. **Information Security Safeguards and Procedures**. This factor refers to the extent and quality of information security [e.g., classified materials controls, open storage rules] in the unit and work location.

1. Work location has very extensive information security safeguards and procedures.
2. Work location has extensive information security safeguards and procedures.
3. Work location has moderately extensive information security safeguards and procedures.
4. Work location has limited information security safeguards and procedures.
5. Work location has very limited information security safeguards and procedures.

D2. **Physical Security Safeguards and Procedures**. This factor refers to the extent and quality of physical security [e.g., facilities and building access controls, exit searches, visibility of guard force, external security measures] in the unit and work location.

1. Work location has very extensive physical security safeguards and procedures (e.g., work place has extensive fixed active (and passive) external security, all building access positively controlled, SCI areas require positive dual control for access, and searches are conducted regularly).
2. Work location has extensive physical security safeguards and procedures (e.g., work place has some fixed active (and passive) external security, general building access is positively controlled, SCI areas require positive dual control for access, and searches are conducted on a random basis).
3. Work location has moderately extensive physical security safeguards and procedures (e.g., work place has no fixed active external security, general building access is controlled, SCI areas require dual control for access, and there are no search procedures).
4. Work location has limited physical security safeguards and procedures (e.g., work place has no fixed external security measures, no positive dual control for access to SCI areas, but general building access is controlled, and no search procedures)
5. Work location has very limited physical security safeguards and procedures (e.g., work place has no fixed external security measures, no positive dual control for access, no designated guard controlling building access, and no search procedures).

D. Security Countermeasures, continued

D3. **Personnel Security Procedures**. This factor refers to the extent and quality of personnel security procedures associated with this position [e.g., personnel security investigations, drug testing, polygraph, continuing evaluation procedures].

1. Work location has very extensive personnel security safeguards and procedures (e.g., position requires single scope background investigation, periodic reinvestigations, initial and periodic counterintelligence polygraph, random lifestyle polygraphs, and other continuing evaluation procedures).
2. Work location has extensive personnel security safeguards and procedures (e.g., position requires single scope background investigation, periodic reinvestigations, initial and periodic counterintelligence polygraphs, and lifestyle polygraph).
3. Work location has moderately extensive personnel security safeguards and procedures (e.g., position requires single scope background investigation, periodic reinvestigations, and initial and periodic counterintelligence polygraphs).
4. Work location has limited personnel security safeguards and procedures (e.g., position requires single scope background investigation, periodic reinvestigations, and initial counterintelligence polygraph).
5. Work location has very limited personnel security safeguards and procedures (e.g., position only requires single scope background investigation and periodic reinvestigations).

D4. **Security Education Procedures**. This factor refers to the extent and quality of security education [e.g., security awareness briefings, threat briefings, counterintelligence briefings] in the organization and work unit.

1. Work location has very extensive security education program or procedures.
2. Work location has extensive security education program or procedures.
3. Work location has moderately extensive security education program or procedures.
4. Work location has limited security education program or procedures.
5. Work location has very limited or no security education program or procedures.

D5. **Employee Assistance Programs**. This factor refers to the extent and quality of employee assistance programs [e.g., alcohol, drug, family, financial, etc.] available to the position holder.

1. Position holder has excellent access to employee assistance programs. Program includes numerous types of assistance. Program use is encouraged, has management support, and has strict confidentiality.
2. Position holder has good access to employee assistance programs. Program includes several types of assistance.
3. Position holder has some access to employee assistance programs. Program includes some types of assistance.
4. Position holder has only limited or inconvenient access to employee assistance programs. Program includes few types of assistance.
5. Position holder does not have access to an employee assistance program. If a program exists, its use is discouraged due to lack of confidentiality and lack of management support.

D. Security Countermeasures, continued

D6. **Availability of Support Systems.** This factor refers to whether there are family members, coworkers, or other English speaking personnel in the geographic location of the position. These persons could provide a support system for position holders by allowing them to discuss interests and problems.

1. Position holder typically has access to many family members, coworkers, and Americans in his/her assigned geographic locations.
2. Position holder typically has access to some family members, some coworkers, and many Americans in his/her assigned geographic locations.
3. Position holder typically has access to some coworkers and many non-American English speaking personnel in his/her assigned geographic locations.
4. Position holder typically has access to only a few coworkers or English speaking personnel in his/her assigned geographic locations.
5. Position holder typically does not have access to family members, and has access to very few or no coworkers or English-speaking personnel in his/her assigned geographic locations.